[c1] A system for providing private messaging among multiple users, comprising:

a packet network;

one or more private messaging agents coupled to the packet network, wherein the private messaging agents handle private messages and corresponding access restrictions messages;

one or more trusted couriers coupled to the packet network and operable to relay the private messages and corresponding access restrictions messages between the private messaging agents, wherein the one or more trusted couriers operate to convey private messages independently from corresponding access restrictions messages.

[c2] The system of claim 1 in which each trusted courier comprises:

a foreground element operable to transfer private messages among the private messaging agents; and

a background element operable to transfer the access restrictions messages and other background signaling among the private messaging agents.

[c3] The system of claim 2, in which the foreground element

comprises:

an account management component operable to manage information defining a relationship between the trusted courier containing the foreground element and each user and private messaging agent to facilitate future interactions.

[c4] The system of claim 2, in which the foreground element comprises:

an information security component, operable to communicate authentication credentials between the foreground element, private messaging agents and other trusted couriers.

[c5] The system of claim 2, in which the background element comprises:

an information security component, operable to communicate authentication credentials between the background element, private messaging agents and other trusted couriers.

[c6] The system of claim 1 in which at least one trusted courier is configured to serve multiple users without any constraint on the domain of their addresses.

[c7] The system of claim 1 in which at least one trusted courier is a private courier that may serve only users

whose address is within the same domain as the trusted courier.

[c8] The system of claim 1 in which exactly one trusted courier is designated as a root courier that is operable to certify the identity of all other trusted couriers

[c9] The system of claim 1 in which at least one trusted courier is designated as a gateway courier that is operable to insulate subordinate trusted couriers from the remainder of the network.

[c10] A trusted courier comprising:
a foreground element operable to transfer private messages to external agents; and
a background element operable to transfer access restrictions messages to external agents.

[c11] The trusted courier of claim 10, in which the foreground element comprises:
an account management component operable to manage information defining a relationship between the trusted courier containing the foreground element and each user and private messaging agent to facilitate future interactions.

[c12] The trusted courier of claim 10 in which the foreground element comprises:

an information security component, operable to communicate authentication credentials between the foreground element, private messaging agents and other trusted couriers.

[c13] The trusted courier of claim 10 in which the background element comprises:
an information security component, operable to communicate authentication credentials between the foreground element, private messaging agents and other trusted couriers.

[c14] A method of providing private messaging services comprising:

sending an Invitation to Register to a prospective user of the private messaging service;
registering a user by establishing an account and agent with key materials for the prospective user;
routing the key material and access restrictions associated with each private message between registered users through the background element of one or more trusted couriers separately from the private messages; and
routing the private messages between registered users through the foreground element of one or more trusted couriers, separately from the content keys and access restrictions.

[c15] A method in accordance with claim 14, in which the act of sending an Invitation comprises:

sending an unencrypted message to an addressee who is not a registered user;

explaining the private messaging service and providing instructions for how to register; and

providing an introduction certificate for encryption and signature verification of a trusted courier offering the private messaging service.

[c16] A method in accordance with claim 14 wherein the act of establishing an account comprises:

presenting a form to the prospective new user containing the messaging address to which Invitation had been sent;

requesting an account password for service access control, user contact information, and billing information;

downloading an Agent installer application program which installs a private messaging Agent to the prospective new user's computer;

executing the Agent installer to install the Agent;

establishing a local password for ensuring that future access to the agent may only be accomplished by the new user;

creating and exchanging between the agent and a

trusted courier a number of cryptographic keys;

storing the keys;

sending an indication that the agent is installed correctly to the trusted courier; and

activating the newly registered user's account in the trusted courier.

[c17] A method in accordance with claim 16 further comprising the acts of:

propagating the newly registered user's account, including all keys, from the foreground element to its corresponding background element.

[c18] A private messaging system implementing the method of claim 14.

[c19] A private messaging system for routing a message between a first agent and a second agent, the system comprising:

a first courier having a trust relationship with the first agent;

a second courier having a trust relationship with the second agent and with the first courier;

wherein the first courier is operable to receive a message identifying the second agent as a recipient from the first agent, determine that the second agent has a trust relationship with the second courier, and

send the message to the second courier using the trust relationship between the first courier and the second courier; and

wherein the second courier is operable to relay the message to the second agent using the trust relationship between the second courier and the second agent.

[c20] The private messaging system of claim 19 wherein at least a portion of the message is encrypted by the first courier using a content encryption key (CEK); and

the CEK is conveyed to the second agent using a communication channel separate from a communication channel used to send and relay the message.

[c21] The private messaging system of claim 19 wherein the second courier is operable to receive messages identifying the first agent as a recipient from the second agent, determine that the first agent has a trust relationship with the first courier, and send the message to the first courier using the trust relationship between the first courier and the second courier; and

wherein the first courier is operable to relay the message to the first agent using the trust relationship between the first courier and the first agent.

[c22] The private messaging system of claim 19 wherein each

trust relationship is provided by cryptographic key/ signature information known only to the agents/couriers that have the trust relationship.

[c23] The private messaging system of claim19 wherein the first and second couriers are unable to decrypt all of the message.

[c24] A method for routing a private message between a sending agent and a recipient agent, the method comprising:

providing a first agent;

providing a second agent;

providing a first courier having knowledge of a number of agents, including the first agent, that are registered with the first courier;

providing a second courier having knowledge of a number of agents, including the second agent, that are registered with the second courier;

providing a private message from the first agent to the first courier, the private message comprising a header and a message ID, wherein the private message header identifies a recipient address of the second agent, and wherein the content is encrypted using a content encryption key (CEK);

signing and encrypting the private message with a first message signing key used by the first agent for messages to the first courier;

sending the signed private message in one or more parts, the signed private message addressed to the first courier, the message comprising the header, message ID, the encrypted content of the private message, and the CEK used to encrypt the content of the private message;

in the first courier, decrypting and validating the private message header using the first message signing key known to the first courier, wherein the private message content remain encrypted by the CEK;

identifying the second courier from the recipient address in the decrypted first message header;

for the at least one registered recipient address in the decrypted message header, reconstructing the message;

signing and encrypting the reconstructed message using a second message signing key used by the first courier for messages to the second courier;

sending the signed and encrypted reconstructed message in one or more parts to the second courier, the signed and encrypted reconstructed message comprising the header, message ID, the encrypted content of the private message, and the CEK used to encrypt the content of the private message;

in the second courier, decrypting and validating the private message header using the second message

signing key known to the second courier, wherein the private message content remain encrypted by the CEK;

identifying the recipient address in the decrypted message header;

signing and encrypting the private message with a third message signing key used by the second agent for messages to the second agent;

sending the signed private message in one or more parts to the second agent the message comprising the header, message ID, the encrypted content of the private message, and the CEK used to encrypt the content of the private message;

decrypting the signed private message in the second agent using the third message signing key; and

decrypting the encrypted content in the second agent using the CEK.

[c25] The method of claim 24 wherein the first courier comprises a foreground component and a background component.

[c26] The method of claim 25 wherein the act of sending the signed private message comprises:

sending a foreground message part from the first agent to the foreground component of the first courier, wherein the foreground message part com-

prises a message body that contains the header, message ID, and CEK-encrypted content of the private message;

sending a background message part from the first agent to the background component of the first courier, wherein the background message part comprises a message body that comprises the header, message ID, and the CEK used to encrypt the content of the private message;

wherein the acts of sending the foreground and background message parts are performed over separate, independent communication channels.

[c27] The method of claim 24 wherein the first courier comprises a foreground component and a background component and the second courier comprises a foreground and a background element.

[c28] The method of claim 27 wherein the act of sending the signed and encrypted reconstructed message comprises:

sending a foreground message part from the first courier foreground component to the foreground component of the second courier, wherein the foreground message part comprises a message body that contains the header, message ID, and CEK-encrypted content of the private message;

sending a background message part from the first

courier background element to the background component of the second courier, wherein the background message part comprises a message body that comprises the header, message ID, and the CEK used to encrypt the content of the private message;

wherein the acts of sending the foreground and background message parts are performed over separate, independent communication channels